PATENT APPLICATION

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of

Michel LINARES

Docket No: Q77862

Appln. No.: 10/677,273

Group Art Unit: 2661

Confirmation No.: 8742

Examiner: Not Yet Assigned

Filed: October 03, 2003

For: A SECURE METHOD OF EXCHANGING INFORMATION MESSAGES

SUBMISSION OF PRIORITY DOCUMENT

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Submitted herewith is a certified copy of the priority document on which a claim to priority was made under 35 U.S.C. § 119. The Examiner is respectfully requested to acknowledge receipt of said priority document.

Respectfully submitted,

Paul F. Neils
Registration No. 33,102

SUGHRUE MION, PLLC
Telephone: (202) 293-7060
Facsimile: (202) 293-7860

WASHINGTON OFFICE
23373
CUSTOMER NUMBER

Enclosure: *French Application No. 0212404, dated October 7, 2003*

Date: January 30, 2004

Attorney Docket No.: Q77862

10/677,273
Michel LINARES
Conf # 8742
Group Art Unit: 2661
Priority doc 1 of 1

R E P U B L I Q U E F R A N Ç A I S E

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

BREVET D'INVENTION

CERTIFICAT D'UTILITÉ - CERTIFICAT D'ADDITION

COPIE OFFICIELLE

Le Directeur général de l'Institut national de la propriété industrielle certifie que le document ci-annexé est la copie certifiée conforme d'une demande de titre de propriété industrielle déposée à l'Institut.

Fait à Paris, le 26 NOV. 2003

Pour le Directeur général de l'Institut
national de la propriété industrielle
Le Chef du Département des brevets

Martine PLANCHE

INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE
SIEGE
26 bis, rue de Saint Petersbourg
75800 PARIS cedex 08
Téléphone : 33 (0)1 53 04 53 04
Télécopie : 33 (0)1 53 04 45 23
www.inpi.fr

ETABLISSEMENT PUBLIC NATIONAL CREE PAR LA LOI N° 51-444 DU 19 AVRIL 1951

1er dépôt

INPI
INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE
26 bis, rue de Saint Pétersbourg
75800 Paris Cedex 08
Téléphone : 01 53 04 53 04 Télécopie : 01 42 94 86 54

BREVET D'INVENTION
CERTIFICAT D'UTILITÉ

cerfa N° 11354*01

Code de la propriété intellectuelle - Livre VI

REQUÊTE EN DÉLIVRANCE 1/2

Important ! Remplir impérativement la 2ème page.

Cet imprimé est à remplir lisiblement à l'encre noire DB 540 W /190600

Réservé à l'INPI

REMISE DES PIÈCES DATE 7 OCT 2002
LIEU 75 INPI PARIS
N° D'ENREGISTREMENT NATIONAL ATTRIBUÉ PAR L'INPI 0212404
DATE DE DÉPÔT ATTRIBUÉE PAR L'INPI - 7 OCT. 2002

1 NOM ET ADRESSE DU DEMANDEUR OU DU MANDATAIRE À QUI LA CORRESPONDANCE DOIT ÊTRE ADRESSÉE

ALSTOM
LEGAL - Intellectual Property
25, avenue Kléber
75116 PARIS/FR

Vos références pour ce dossier *(facultatif)* A30394/PB/IB

Confirmation d'un dépôt par télécopie ☐ N° attribué par l'INPI à la télécopie

2 NATURE DE LA DEMANDE	Cochez l'une des 4 cases suivantes
Demande de brevet	☒
Demande de certificat d'utilité	☐
Demande divisionnaire	☐
Demande de brevet initiale	N° Date / /
ou demande de certificat d'utilité initiale	N° Date / /
Transformation d'une demande de brevet européen *Demande de brevet initiale*	☐ N° Date / /

3 TITRE DE L'INVENTION (200 caractères ou espaces maximum)

Procédé d'échange sécuritaire de messages d'information.

4 DÉCLARATION DE PRIORITÉ OU REQUÊTE DU BÉNÉFICE DE LA DATE DE DÉPÔT D'UNE DEMANDE ANTÉRIEURE FRANÇAISE	
	Pays ou organisation Date / / N°
	Pays ou organisation Date / / N°
	Pays ou organisation Date / / N°
	☐ S'il y a d'autres priorités, cochez la case et utilisez l'imprimé «Suite»

5 DEMANDEUR		☐ S'il y a d'autres demandeurs, cochez la case et utilisez l'imprimé «Suite»
Nom ou dénomination sociale		ALSTOM
Prénoms		
Forme juridique		S.A.
N° SIREN		
Code APE-NAF		
Adresse	Rue	25, avenue Kléber
	Code postal et ville	75116 PARIS
Pays		FRANCE
Nationalité		Française
N° de téléphone *(facultatif)*		01 47 55 21 00
N° de télécopie *(facultatif)*		
Adresse électronique *(facultatif)*		

1er dépôt

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

BREVET D'INVENTION
CERTIFICAT D'UTILITÉ

REQUÊTE EN DÉLIVRANCE 2/2

7 OCT 2002
Réservé à l'INPI
REMISE DES PIÈCES
DATE
75 INPI PARIS
LIEU
0212404
N° D'ENREGISTREMENT
NATIONAL ATTRIBUÉ PAR L'INPI

DB 540 W /190600

Vos références pour ce dossier : *(facultatif)*		A30394/PB/IB
6 **MANDATAIRE**		
Nom		GOSSE
Prénom		Michel
Cabinet ou Société		c/o ALSTOM LEGAL -Intellectual Property
N °de pouvoir permanent et/ou de lien contractuel		
Adresse	Rue	25, avenue Kléber
	Code postal et ville	75116 PARIS
N° de téléphone *(facultatif)*		01 47 55 20 00
N° de télécopie *(facultatif)*		01 47 55 23 57
Adresse électronique *(facultatif)*		
7 **INVENTEUR (S)**		
Les inventeurs sont les demandeurs		☐ Oui ☒ Non **Dans ce cas fournir une désignation d'inventeur(s) séparée**
8 **RAPPORT DE RECHERCHE**		**Uniquement pour une demande de brevet (y compris division et transformation)**
Établissement immédiat ou établissement différé		☒ ☐
Paiement échelonné de la redevance		**Paiement en deux versements, uniquement pour les personnes physiques** ☐ Oui ☒ Non
9 **RÉDUCTION DU TAUX DES REDEVANCES**		**Uniquement pour les personnes physiques** ☐ Requise pour la première fois pour cette invention *(joindre un avis de non-imposition)* ☐ Requise antérieurement à ce dépôt *(joindre une copie de la décision d'admission pour cette invention ou indiquer sa référence) :*
Si vous avez utilisé l'imprimé «Suite», indiquez le nombre de pages jointes		

10 **SIGNATURE DU DEMANDEUR OU DU MANDATAIRE (Nom et qualité du signataire)** Michel GOSSE, Ingénieur	**VISA DE LA PRÉFECTURE OU DE L'INPI** L. MARIELLO

La loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés s'applique aux réponses faites à ce formulaire.
Elle garantit un droit d'accès et de rectification pour les données vous concernant auprès de l'INPI.

L'invention se rapporte à un procédé d'échange sécuritaire de messages d'information envoyés successivement, à intervalles de temps donnés, d'une plate-forme émettrice vers une plate-forme réceptrice. L'invention concerne plus particulièrement un procédé permettant de s'assurer que le dernier message capté par la plate-forme réceptrice correspond au dernier message envoyé par la plate-forme émettrice.

Le procédé selon l'invention trouve notamment une application dans les systèmes de conduite et/ou de supervision de trains, dénommés SACEM (pour "système d'Aide à la Conduite, à l'Exploitation et à la Maintenance") comprenant un poste de commande centralisé, des installations fixes le long des voies et un équipement de commande dans chaque train. Dans de tels systèmes de conduite, le poste de commande centralisé transmet, à intervalles de temps réguliers, des messages d'information aux installations fixes, ces messages comportant des informations relatives aux conditions de circulation sur un ou plusieurs cantons de voie situés en aval de l'installation fixe. L'équipement de commande de tout train se trouvant sur le réseau reçoit alors, des installations fixes, le dernier message d'information reçu par l'installation fixe et en déduit la vitesse de marche à adopter. Lors de l'échange de tels messages d'information il est indispensable, pour des questions de sécurité, d'être sûr que le dernier message reçu par les installations fixes correspond bien au dernier message d'information envoyé par le poste de commande centralisé. Or, compte tenu des différents composants intervenant dans la transmission des messages et de la distance relativement importante pouvant exister entre le poste de commande centralisé et les installations fixes, il est possible que certains messages soient perturbés et retardés dans leur transmission et parviennent tardivement aux installations fixes provoquant ainsi une modification de l'ordre de réception des messages d'information par l'installation fixe par rapport à l'ordre d'émission par le poste de commande centralisé. Dans un tel cas le message d'information actualisé au niveau de l'installation fixe ne correspond plus au dernier message réellement envoyé par le poste de commande centralisé. Bien que de tels phénomènes soient rares, ils doivent absolument être détectés pour assurer la sécurité du trafic.

Classiquement, il est connu pour sécuriser la transmission des messages d'information, d'effectuer des échanges bidirectionnels et permanents des données de sorte que le message d'information reçu par l'installation fixe soit réémis vers le poste de commande centralisé qui s'assure de sa correspondance avec le message d'information envoyé. Toutefois, de tels procédés utilisant des échanges bidirectionnels des données mettent en œuvre des procédés de traitements complexes nécessitant des dispositifs coûteux à l'arrivée et au départ.

Le but de la présente invention est donc de proposer un procédé d'échange sécuritaire de messages d'information qui permette de s'assurer, lors d'échanges successifs unidirectionnels de messages d'information entre une plate-forme émettrice et une plate-forme réceptrice, que le dernier message capté par la plate-forme réceptrice correspond bien au dernier message envoyé par la plate-forme émettrice afin de pouvoir valider la bonne actualisation du message d'information au niveau de la plate-forme réceptrice.

A cet effet, l'invention a pour objet un procédé d'échange sécuritaire de messages d'information envoyés successivement d'une plate-forme émettrice vers une plate-forme réceptrice, caractérisé en ce qu'il comporte :

a) une séquence d'initialisation dans laquelle au moins un message d'initialisation contenant l'information relative à la date t_I d'envoi du premier message d'information M_I est échangé entre la plate-forme émettrice et la plate forme réceptrice de sorte que les plates-formes émettrice et réceptrice connaissent alors, l'une et l'autre, la date d'envoi t_I du premier message d'information M_I.

b) une séquence de transmission des messages d'information dans laquelle :

- les messages d'information sont envoyés successivement par la plate-forme émettrice à intervalles de temps ΔT_E donnés avec une tolérance temporelle d'émission δ ($\delta < \Delta T_E$), en se basant sur une horloge propre à la plate-forme émettrice, de sorte que le premier message M_I est émis à la date t_I de l'horloge et le $n^{ième}$ message M_n est envoyé à la date $t_n=t_I+(n-1)*\Delta T_E+\delta$, chaque message M_n étant codé au moyen d'un code dynamique C_n propre à

la date t_n d'envoi du message. Avantageusement, les données des messages d'information sont par ailleurs codées par un codage défini selon les critères de sécurité de l'application, afin de rendre les messages d'information incompréhensibles en cas de dysfonctionnement de la transmission. Ce codage est par exemple le codage SACEM.

- les messages reçus par la plate-forme réceptrice sont traités en fonction de leur date de réception t_r en se basant sur une horloge propre à la plate-forme réceptrice de sorte que les messages reçus dans une fenêtre d'observation F_n au voisinage de t_n sont décodés avec une séquence de décodage DC_n adaptée pour décoder le code dynamique C_n, l'horloge de la plate-forme réceptrice étant calée à la date t_1 à la réception du premier message M_1.

Selon des modes particuliers de réalisation, le procédé selon l'invention peut comprendre l'une ou plusieurs des caractéristiques suivantes prises isolément ou selon toutes les combinaisons techniquement possibles :

- lors de la séquence d'initialisation a), d'une part un message d'initialisation M_0 codé est envoyé depuis la plate-forme émettrice vers la plate-forme réceptrice, et d'autre part un message d'initialisation M'_0 codé est envoyé depuis la plate-forme réceptrice vers la plate-forme émettrice, ces messages d'initialisation M_0, M'_0 contenant l'information relative à la date t_1 d'envoi du premier message d'information M_1, les dits messages d'initialisation M_0, M'_0 étant décodés par les plates-formes émettrice et réceptrice qui connaissent alors de la date d'envoi t_1 du premier message d'information M_1 ;
- en cas de non-réception du premier message M_1 dans un temps alloué après la réception du message d'initialisation, l'horloge de la plate-forme émettrice est automatiquement calée à la date t_1 à l'instant correspondant à la fin du temps alloué ;
- la fenêtre d'observation Fn correspond à une fenêtre de temps $[t_1+(n-1)*\Delta T_E-\Delta T_F*\varepsilon,\ t_1+(n-1)*\Delta T_E+\Delta T_F*(1-\varepsilon)]$, où n est un nombre entier et ΔT_F correspond à la largeur de la fenêtre d'observation et répond à la relation $\Delta T_F \leq \Delta T_E$, et où ε est compris entre 0 et 1 ;

- un signal de synchronisation d'horloge est émis régulièrement par la plate-forme émettrice, entre l'émission des messages M_n, ce signal de synchronisation étant utilisé pour corriger dynamiquement la fréquence ou la phase de l'horloge interne de la plate-forme réceptrice afin de réduire l'écart de phase ou de fréquence entre les horloges internes des plates-formes réceptrice et émettrice ;
- les messages d'information décodés par la plate-forme réceptrice sont transmis à un module de traitement de l'information ;
- les messages reçus par la plate-forme réceptrice au cours d'une fenêtre d'observation F_n sont stockés de façon séquentielle dans une mémoire ne pouvant stocker qu'un seul message à la fois et en ce que seul le message stocké dans cette mémoire à la fin de la fenêtre d'observation F_n est transmis au module de traitement de l'information ;
- la plate-forme émettrice appartient à un poste de commande centralisé d'un système de supervision et de conduite du trafic ferroviaire et la plate-forme réceptrice appartient à une installation fixe disposée en bordure d'une voie ferrée et en ce que le module de traitement de l'information est constitué d'un équipement de commande disposé à bord d'un train circulant sur un canton de voie associé à l'installation fixe.

On comprendra mieux les buts, aspects et avantages de la présente invention, d'après la description donnée ci-après d'un mode particulier de réalisation de l'invention, présenté à titre d'exemple non limitatif, en se référant aux dessins annexés, dans lesquels :

- la figure 1 est représentation partielle et schématique d'une installation de supervision de trains équipée d'un procédé d'échange sécuritaire de message d'information selon l'invention .
- la figure 2 est un organigramme représentant les principales étapes du procédé d'émission mis en œuvre par la plate-forme émettrice conformément au procédé d'échange sécuritaire selon l'invention.
- la figure 3 est un organigramme représentant les principales étapes du procédé de traitement mis en œuvre par la plate-forme réceptrice conformément au procédé d'échange sécuritaire selon l'invention.

- la figure 4 illustre sur une échelle temporelle, l'émission de messages d'information depuis une plate-forme émettrice et la réception des messages sur une plate-forme réceptrice et leur traitement conformément au procédé d'échange sécuritaire selon l'invention.

Pour faciliter la lecture du dessin, seuls les éléments nécessaires à la compréhension de l'invention ont été représentés. Les mêmes éléments portent les mêmes références d'une figure à l'autre.

La figure 1 représente schématiquement un poste de commande centralisé 1 communiquant des messages d'information à des installations fixes 2 disposées en bordure d'un canton de voie ferrée, ces messages comportant des informations relatives aux conditions de circulation sur un ou plusieurs cantons de voie situés en aval de l'installation fixe 2. Ces messages sont ensuite transmis depuis les installations fixes 2 vers un train 5 de manière connue par un circuit de voie, le train 5 comportant un équipement de commande 6 utilisant ces messages d'information pour déterminer notamment la marche à suivre, telle que la vitesse à adopter ou la nécessité de déclencher un arrêt d'urgence.

Pour effectuer la transmission des messages d'information, le poste de commande centralisé 1 comporte une plate-forme émettrice 10 reliée par des câbles de transmission 4 à une plate-forme réceptrice 20 disposée dans l'installation fixe 2. Chaque plate-forme émettrice 10 et réceptrice 20 comporte une horloge interne.

La séquence d'émission des messages d'information par la plate-forme émettrice 10 dans le procédé d'échange sécurisé selon l'invention va maintenant être décrite en relation avec la figure 2.

Conformément à cette figure, dans une première étape 101 du procédé d'échange sécuritaire, une séquence d'initialisation est effectuée au cours de laquelle un message d'initialisation M_0 codé est transmis du poste de la plate-forme émettrice 10 à la plate-forme réceptrice 20. Ce message M_0 contient une partie de l'information de la date initiale du premier message d'information, générée par la plate-forme émettrice, par exemple un nombre aléatoire. Dans une deuxième étape 102, la plate-

forme émettrice reçoit le message M'_0 qui est émis par la plate-forme réceptrice. Ce message M'_0 contient une partie de l'information de la date initiale du premier message d'information, générée par la plate-forme réceptrice, par exemple un nombre aléatoire. Ces messages M_0, M'_0 sont décodés, dans une étape 103 par la plate-forme émettrice 10 pour générer la date initiale du premier message. Eventuellement une partie implicite complète cette date initiale.

La sécurité de transmission de la séquence d'initialisation est assurée classiquement par un échange bidirectionnel permettant de s'assurer de la bonne corrélation entre le message reçu et le message envoyé.

La séquence d'initialisation précédemment décrite est suivie d'une étape 104 du procédé dans laquelle aucun message n'est envoyé par la plate-forme émettrice 10 jusqu'à ce que le temps t_e de l'horloge interne de la plate-forme émettrice 10 atteigne la date t_1 prévue pour l'envoi du premier message M_1. A la date t_1, la plate-forme émettrice 10 envoie le premier message M_1, des messages étant ensuite envoyés à intervalle de temps ΔT_E constant de sorte que le $n^{ième}$ message M_n est envoyé à la date $t_n=t_1+(n-1)*\Delta T_E+\delta$, n étant un nombre entier, δ est la tolérance temporelle d'émission ($\delta < \Delta T_E$).

Selon une caractéristique de l'invention, chaque message M_n envoyé est codé avec un code dynamique C_n propre à la date d'envoi t_n du message. Ce code dynamique C_n est du type choisi parmi les codes dynamiques connus qui possèdent des propriétés de codage telles que le décodage du message M_n avec une séquence de décodage autre que la séquence de décodage DC_n prévue pour décoder le code C_n conduit à l'obtention d'un message incompréhensible grâce au codage défini au niveau de l'application. A titre d'exemple, le codage choisi est une surimposition d'une séquence pseudo-aléatoire basée sur le polynôme primitif $X^{32} + X^{22} + X^2 + X + 1$ appliquée à chacun des bits des données.

Le traitement effectué parallèlement par la plate-forme réceptrice 20, lors de la séquence de transmission des messages d'information par la plate-forme émettrice 10, va maintenant être décrit en relation avec la figure 3.

Conformément à la figure 3, la plate-forme réceptrice 20 reçoit, dans une première étape 201 du procédé, le message M_0 contenu dans la séquence d'initialisation émise par la plate-forme émettrice lors de l'étape 101. Dans une deuxième étape 202, la plate-forme réceptrice 20 émet le message M'_0 qui est reçu par la plate-forme émettrice lors de l'étape 102. Dans une étape 203, ces messages M_0, M'_0 sont décodés par la plate-forme réceptrice 20, pour obtenir la date initiale t1 du premier message M_1, comme dans l'étape 103 pour la plate-forme émettrice.

Dans une étape 204 suivante du procédé déclenchée lorsque la plate-forme réceptrice 20 reçoit le premier message M_1, l'horloge interne de la plate-forme réceptrice 20 est calée sur la date t_1 de sorte que $t_r=t_1$ à l'instant de réception de ce premier message M_1, où t_r est le temps sur l'horloge interne de la plate-forme réceptrice 20. L'horloge interne de la plate-forme réceptrice 20 est également calée par défaut sur la date t_1, si le premier message M_1 ne parvient pas à la plate-forme réceptrice 20 dans un temps alloué après la réception du message d'initialisation M_0.

De manière préférentielle, après la réception du message t_1, l'horloge de la plate-forme réceptrice 20 est synchronisée régulièrement sur l'horloge de la plate-forme émettrice 10 à partir de trames de synchronisation d'horloge émises régulièrement par la plate-forme émettrice 10 au même cycle que les messages M_n. Ces trames sont soit spécifiques ou constituées des messages M_n eux-mêmes. Ainsi, lorsqu'un écart de synchronisation (phase, fréquence, moyenne, moindres carrés ...) est mesuré entre l'horloge interne de la plate-forme émettrice 10 et l'horloge interne de la plate-forme réceptrice 20, une correction de la fréquence ou de la phase de l'horloge interne de la plate-forme réceptrice 20 est réalisée dynamiquement de sorte de réduire l'écart de phase ou de fréquence entre les deux horloges.

Au cours de l'étape suivante 205 du procédé, le premier message M_1 reçu est décodé au moyen d'une séquence de décodage DC_1 adaptée pour décoder le code dynamique C_1 et le résultat du message M_1 décodé est transmis par la plate-forme réceptrice 20 au circuit de voie.

L'étape 206 suivante du procédé est déclenchée de manière itérative lorsque la plate-forme réceptrice 20 reçoit un nouveau message $M_?$, à priori le message M_n, à un instant t_r compris dans une fenêtre d'observation temporelle F_n correspond à une fenêtre de temps $[t_l+(n-1)*\Delta T_E - \Delta T_F*\varepsilon,\ t_l+(n-1)*\Delta T_E + \Delta T_F*(1-\varepsilon)]$, où ΔT_F est la largeur de la fenêtre d'observation, n est un nombre entier et ε est compris entre 0 et 1.

Au cours de l'étape 207 suivante du procédé, le message $M_?$ reçu dans une fenêtre d'observation F_n de la plate-forme émettrice 20 est décodé au moyen d'une séquence de décodage DC_n affectée à cette fenêtre d'observation F_n et correspondant à la séquence codage inverse DC_n adaptée pour décoder uniquement le code dynamique C_n du $n^{ième}$ message émis par la plate-forme émettrice 10.

Dans un mode de réalisation préférentiel de l'invention, le message $M_?$ décodé par la plate-forme réceptrice 20 est alors, dans une étape non représentée sur la figure 3, stocké temporairement dans une mémoire possédant une capacité permettant de ne stocker qu'un seul message à la fois, avant d'être envoyé au circuit de voie à l'instant t_r correspondant à la fin de la fenêtre d'observation F_n. Dans une variante simplifiée, le message $M_?$ peut également être transmis au circuit de voie dès la fin de l'étape 207, sans être stocké dans une mémoire.

Le train 5 se trouvant sur le canton de voie reçoit alors, par l'intermédiaire du circuit de voie, les messages décodés par la plate-forme réceptrice 20 avec l'assurance que les messages $M_?$ reçus devenus compréhensibles grâce au décodage défini au niveau de l'application sont des messages M_n correctement actualisés, dont il faut prendre en compte les informations. Par ailleurs, pour assurer la sécurité de la circulation des trains sur la voie, il est prévu que l'équipement de commande 6 à bord du train 5 déclenche un arrêt d'urgence lorsque le train 5 reçoit successivement plusieurs messages incompréhensibles, par exemple cinq messages de suite, de sorte que le train s'arrête lorsqu'il n'est plus suffisamment renseigné sur les conditions de circulation du canton de voie en aval.

La figure 4 illustre, à titre d'exemple, une séquence d'échange de messages d'information conformément au procédé selon l'invention. Sur cette figure, l'émission des messages M_1 à M_6 est représentée sur l'axe supérieur t_e, cet axe correspondant à l'écoulement du temps sur l'horloge interne de la plate-forme émettrice 10, et la réception des messages est représentée sur l'axe t_r correspondant à l'écoulement du temps sur l'horloge de la plate-forme réceptrice 20. On considérera pour l'exemple décrit à la figure 4 que la séquence d'initialisation, non représentée sur la figure, est initiée à l'instant t_e=4h59mn et que la date t_1 d'envoi du premier message est t_1=5h. L'intervalle ΔT_E est de l'ordre de quelques millisecondes, par exemple ΔT_E=50 ms, de sorte que la mise à jour des messages d'information soit régulière. Dans l'exemple représenté, la tolérance temporelle d'émission δ est nulle et les fenêtres d'observation F_n présentent les caractéristiques ε=0,5 et ΔT_F=25ms.

Ainsi, en se reportant à la figure 4 et notamment à la réception des messages sur l'axe inférieur t_r représentant l'écoulement du temps au niveau de l'horloge de la plate-forme réceptrice 20, quelques instants après l'émission du message M_1 la plate-forme réceptrice 20 reçoit le premier message M_1. La plate-forme réceptrice 20 procède alors au calage de son horloge interne de sorte que t_r=t_1 à l'instant de réception du message M_1. Le message M_1 est ensuite décodé par la plate-forme réceptrice au moyen de la séquence de décodage DC_1 puis est transmis au circuit de voie et donc à un éventuel train 5 présent sur le canton de voie.

Quelques instants plus tard, la plate-forme réceptrice 20 reçoit le message M_2 dans la fenêtre d'observation F_2 centrée sur t_2 et de largeur ΔT_F. La plate-forme réceptrice 20 procède alors au décodage du message M_2 avec la séquence de décodage DC_2 . Ce message décodé est stocké dans une mémoire de la plate-forme réceptrice possédant une capacité permettant de ne stocker qu'un seul message à la fois puis est transmis au circuit de voie à l'instant t_r correspondant à la fin de la fenêtre d'observation F_2 soit $t_r = t_2 + \Delta T_F/2$. L'équipement de commande 6 du train 5 se trouvant sur le canton de voie est alors renseigné par le message M_2 sur les conditions de circulation.

Au cours de la fenêtre d'observation F_3, aucun message n'est reçu par la plate-forme réceptrice 20, suite à des perturbations dans la transmission du message M_3 Dans ce

cas, le message transmis par la plate-forme réceptrice 20 au circuit de voie à l'instant t_r correspondant à la fin de la fenêtre d'observation F_3, est incompréhensible grâce au codage de l'application, de sorte que l'équipement de commande 6 du train 5 se trouvant sur le canton de voie soit renseigné sur ce défaut d'actualisation des messages d'information.

Le message M_3 étant finalement reçu dans la fenêtre d'observation F_4, ce message M_3 est alors décodé avec la séquence de décodage DC_4 affecté à la fenêtre F_4 ce qui conduit à l'obtention d'un message décodé incompréhensible grâce au codage de l'application qui est stocké dans la mémoire de la plate-forme réceptrice 20. Ce message incompréhensible est transmis au circuit de voie à l'instant t_r correspondant à la fin de la fenêtre d'observation F_4 et l'équipement de commande 6 du train 5 reçoit ce message incompréhensible qu'il interprète comme un nouveau défaut d'actualisation des messages d'information. L'équipement de commande 6 comptabilise alors deux défauts successifs d'actualisation des messages d'information mais ne provoque pas encore d'arrêt d'urgence du train si la tolérance permise est de cinq défauts successifs.

Au cours de la fenêtre d'observation F_5, deux messages M_4 et M_5 sont successivement reçus par la plate-forme réceptrice 20. Dans un premier temps la plate-forme réceptrice 20 reçoit le message M_4 puis le message M_5 dans la même fenêtre d'observation F_5. La plate-forme réceptrice procède au décodage de ce dernier message M_5, au moyen de la séquence de décodage DC_5 aboutissant à l'obtention d'un message décodé à nouveau compréhensible grâce au codage de l'application, qui est stocké dans la mémoire de la plate-forme réceptrice 20 à la place du précédent message. Ce message M_5 est transmis au circuit de voie à l'instant t_r correspondant à la fin de la fenêtre d'observation F_5. L'équipement de commande 6 du train 5 reçoit alors un message compréhensible grâce au codage de l'application, le message M_5 avec l'assurance que les informations contenues dans ce message sont des informations correctement actualisées.

Au cours de la fenêtre d'observation F_6, la plate-forme réceptrice 20 reçoit le message M_6 qui est décodé par la séquence de décodage DC_6 puis stocké dans la

mémoire avant d'être envoyé au circuit à l'instant t_r correspondant à la fin de la fenêtre F_6. L'équipement de commande 6 du train 5 reçoit alors un message compréhensible grâce au codage de l'application, le message M_6 avec l'assurance que les informations contenues dans ce message sont des informations actualisées.

Ainsi, un tel procédé de transmission d'échange sécuritaire de messages d'information permet, par un échange régulier unidirectionnel de messages entre une plate-forme émettrice et une plate-forme réceptrice, de garantir la bonne actualisation des messages d'information qui parviennent de façon compréhensible au destinataire et ceci sans faire appel à des moyens de traitement complexes. Un tel procédé présente l'avantage d'être peu coûteux à mettre en œuvre et de permettre une grande vitesse de transmission des informations à l'inverse des systèmes de transmission bidirectionnels habituels dans lequel la séquence de vérification de l'information ralentie considérablement la transmission des messages et donc leur prise en compte. Le procédé selon l'invention permet donc d'avoir une grande cadence de rafraîchissement des messages d'information reçu par le train.

Bien entendu, l'invention n'est nullement limitée au mode de réalisation décrit et illustré qui n'a été donné qu'à titre d'exemple. Des modifications restent possibles, notamment du point de vue de la constitution des divers éléments ou par substitution d'équivalents techniques, sans sortir pour autant du domaine de protection de l'invention.

REVENDICATIONS

1) Procédé d'échange sécuritaire de messages d'information envoyés successivement d'une plate-forme émettrice (10) vers une plate-forme réceptrice (20), caractérisé en ce qu'il comporte :

a) une séquence d'initialisation dans laquelle au moins un message d'initialisation contenant l'information relative à la date t_1 d'envoi du premier message d'information M_1 est échangé entre la plate-forme émettrice (10) et la plate-forme réceptrice (20) de sorte que les dites plates-formes émettrice (10) et réceptrice (20) connaissent alors la date d'envoi t_1 du premier message d'information M_1.

b) une séquence de transmission des messages d'information dans laquelle :

- les messages d'information sont envoyés successivement par la plate-forme émettrice (10) à intervalles de temps ΔT_E donnés avec une tolérance temporelle d'émission δ, en se basant sur une horloge propre à la plate-forme émettrice (10), de sorte que le premier message M_1 est émis à la date t_1 de la dite horloge et le $n^{ième}$ message M_n est envoyé à la date $t_n=t_1+(n-1)*\Delta T_E+\delta$, chaque message M_n étant codé au moyen d'un code dynamique C_n propre à la date t_n d'envoi du dit message ;

- les messages reçus par la plate-forme réceptrice (20) sont traités en fonction de leur date de réception t_r en se basant sur une horloge propre à la plate-forme réceptrice (20) de sorte que les messages reçus dans une fenêtre d'observation F_n au voisinage de t_n sont décodés avec une séquence de décodage DC_n adaptée pour décoder le code dynamique C_n, la dite horloge de la plate-forme réceptrice (20) étant calée à la date t_1 à la réception du premier message M_1.

2) Procédé d'échange sécuritaire de messages d'information selon la revendication 1, caractérisé en ce que lors de la séquence d'initialisation a), d'une part un message d'initialisation M_0 codé est envoyé depuis la plate-forme émettrice (10) vers la plate-forme réceptrice (20), et d'autre part un message d'initialisation M'_0 codé est envoyé depuis la plate-forme réceptrice (20) vers la plate-forme émettrice

(10), ces messages d'initialisation M_0, M'_0 contenant l'information relative à la date t_1 d'envoi du premier message d'information M_1, les dits messages d'initialisation M_0, M'_0 étant décodés par les plates-formes émettrice (10) et réceptrice (20) qui connaissent alors de la date d'envoi t_1 du premier message d'information M_1.

3) Procédé d'échange sécuritaire de messages d'information selon l'une quelconque des revendications 1 à 2, caractérisé en ce qu'en cas de non-réception du premier message M_1 dans un temps alloué après la réception du message d'initialisation, l'horloge de la plate-forme émettrice (20) est automatiquement calée à la date t_1 à l'instant correspondant à la fin du temps alloué.

4) Procédé d'échange sécuritaire de messages d'information selon l'une quelconque des revendications 1 à 3, caractérisé en ce que la dite fenêtre d'observation F_n correspond à une fenêtre de temps $[t_1+(n-1)*\Delta T_E-\Delta T_F*\varepsilon,\ t_1+(n-1)*\Delta T_E+\Delta T_F*(1-\varepsilon)]$, où ΔT_F correspond à la largeur de la fenêtre d'observation et répond à la relation $\Delta T_F \leq \Delta T_E$ et où ε est compris entre 0 et 1.

5) Procédé d'échange sécuritaire de messages d'information selon l'une quelconque des revendications 1 à 4, caractérisé en ce qu'un signal de synchronisation d'horloge est émis régulièrement par la plate-forme émettrice (10), entre l'émission des messages M_n, ce signal de synchronisation étant utilisé pour corriger dynamiquement la fréquence ou la phase de l'horloge interne de la plate-forme réceptrice (20) afin de réduire l'écart de phase ou de fréquence entre les horloges internes des plates-formes réceptrice (20) et émettrice (10).

6) Procédé d'échange sécuritaire de messages d'information selon l'une quelconque des revendications 1 à 5, caractérisé en ce que les messages d'information décodés par la plate forme réceptrice (20) sont transmis à un module de traitement de l'information (6).

7) Procédé d'échange sécuritaire de message d'information selon l'une quelconque des revendications 1 à 6, caractérisé en ce que les messages reçus par la plate-forme réceptrice (20) au cours d'une fenêtre d'observation F_n sont stockés de

façon séquentielle dans une mémoire ne pouvant stocker qu'un seul message à la fois et en ce que seul le message stocké dans cette mémoire à la fin de la dite fenêtre d'observation F_n est transmis au module de traitement de l'information (6).

8) Procédé d'échange sécuritaire de message d'information selon l'une quelconque des revendications 1 à 7, caractérisé en ce que la plate-forme émettrice (10) appartient à un poste de commande centralisé (1) d'un système de supervision et de conduite du trafic ferroviaire et la plate-forme réceptrice (20) appartient à une installation fixe (2) disposée en bordure d'une voie ferrée et en ce que le dit module de traitement de l'information (6) est constitué d'un équipement de commande disposé à bord d'un train (5) circulant sur un canton de voie associé à la dite installation fixe (2).

1 / 3

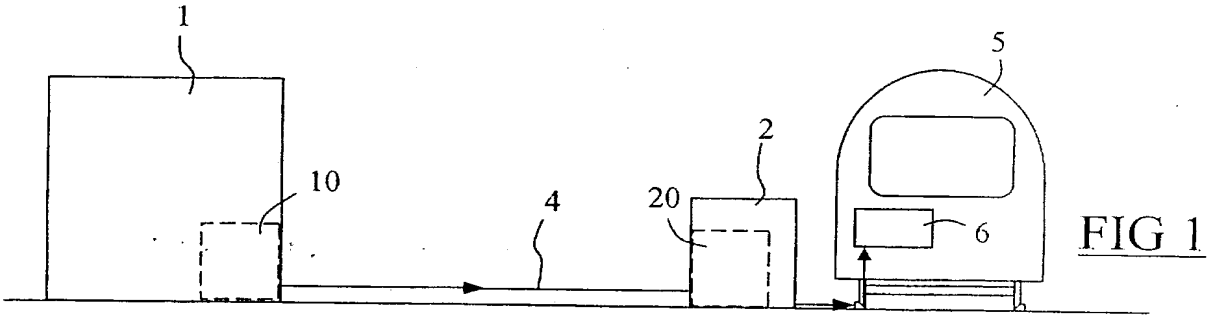

1
10
4
20
2
5
6

FIG 1

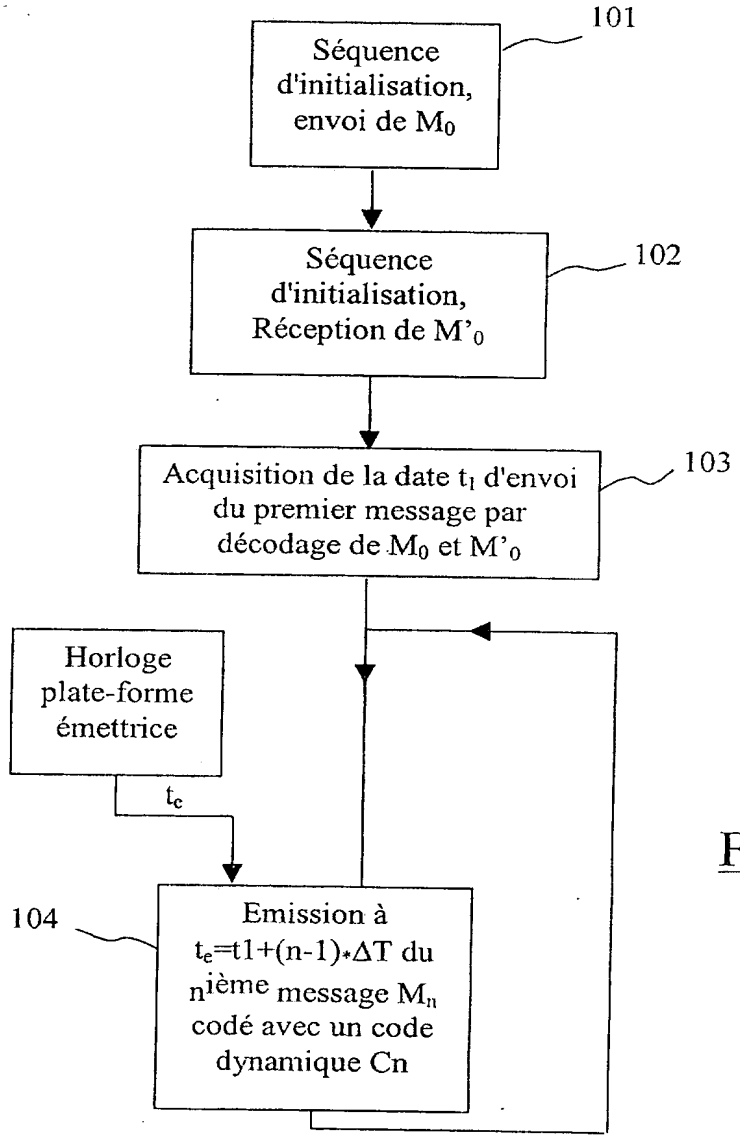

Séquence d'initialisation, envoi de M_0
101
Séquence d'initialisation, Réception de M'_0
102
Acquisition de la date t_1 d'envoi du premier message par décodage de M_0 et M'_0
103
Horloge plate-forme émettrice
t_e
Emission à $t_e=t1+(n-1)*\Delta T$ du $n^{ième}$ message M_n codé avec un code dynamique Cn
104

FIG 2

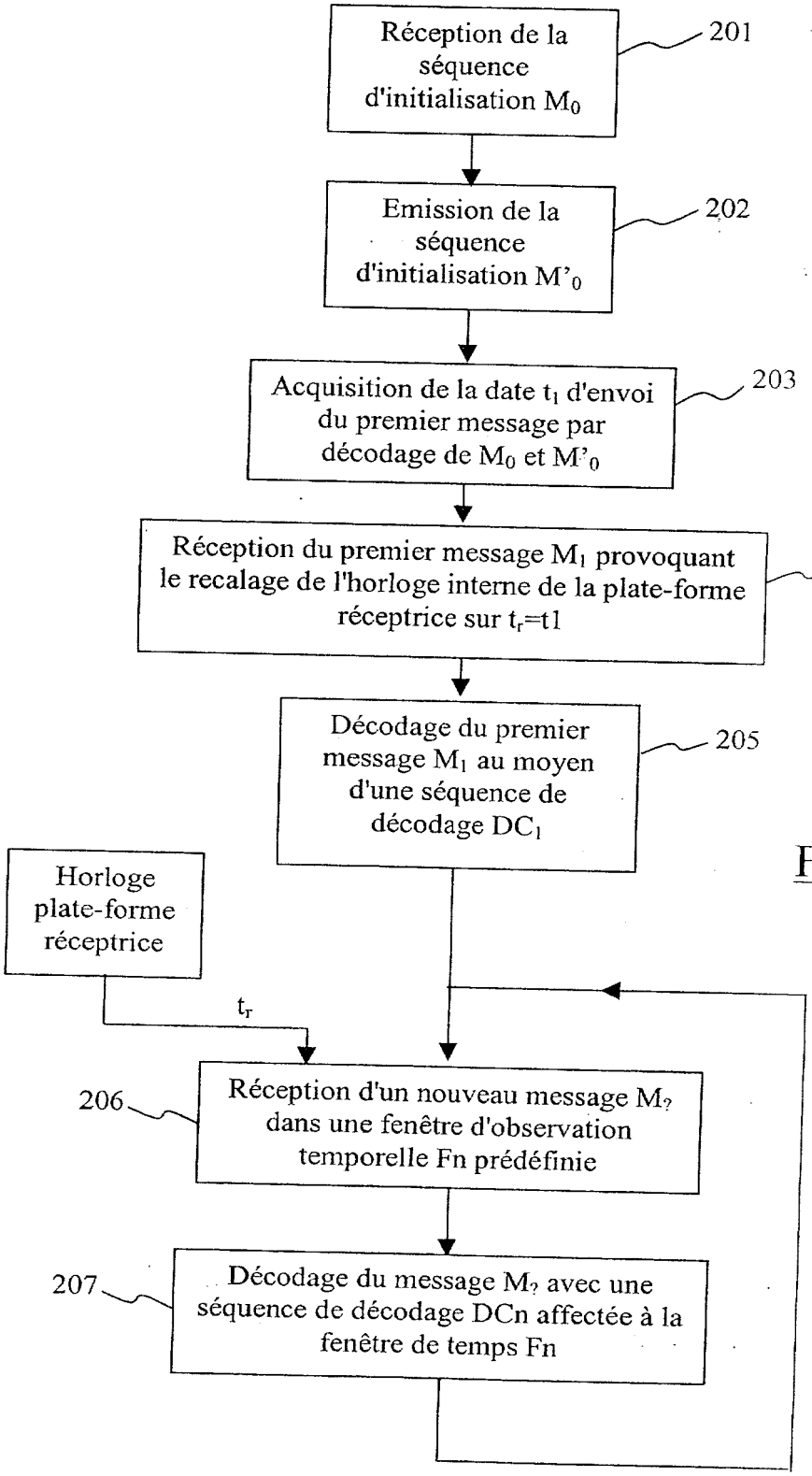
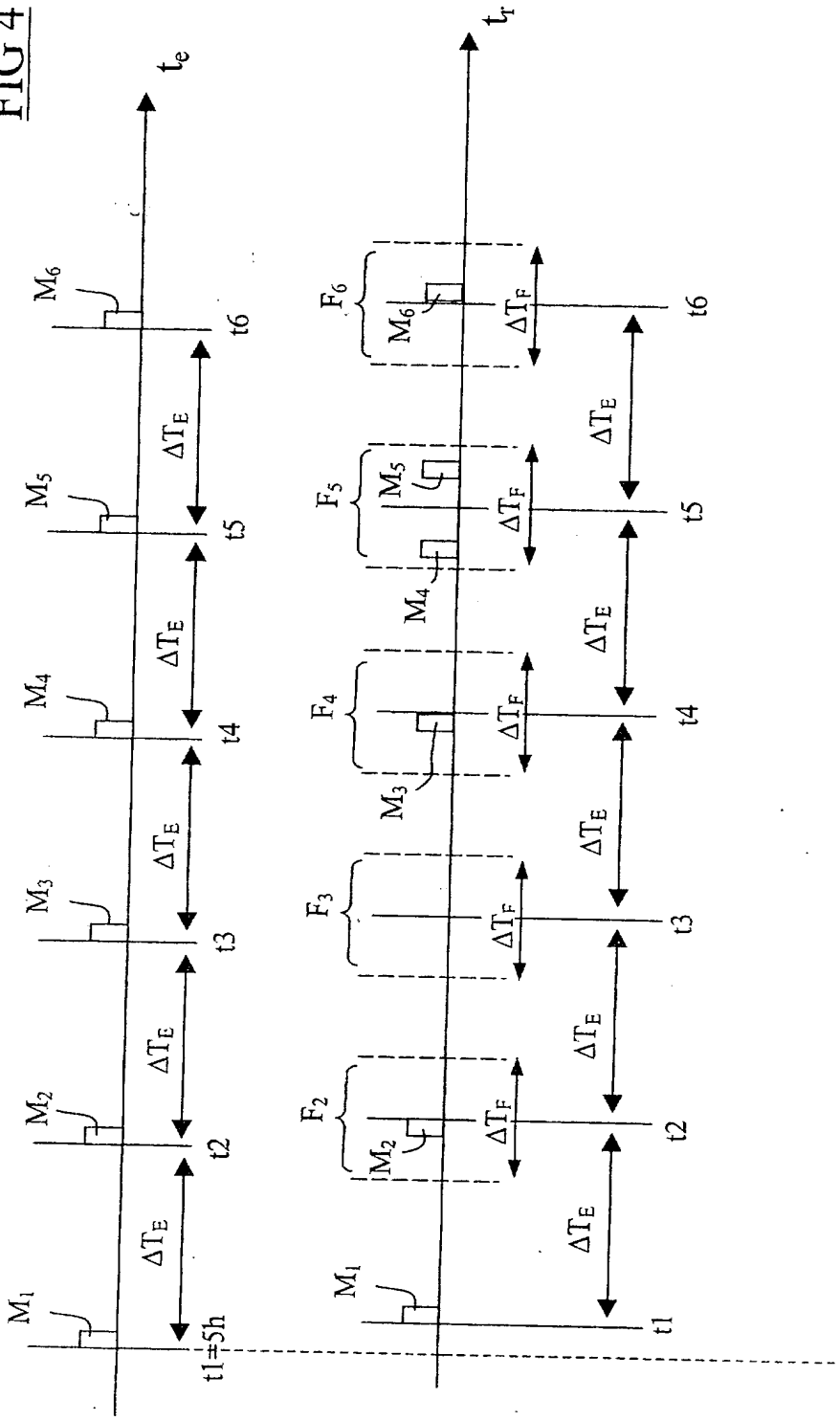

Réception de la séquence d'initialisation M_0
201
Emission de la séquence d'initialisation M'_0
202
Acquisition de la date t_1 d'envoi du premier message par décodage de M_0 et M'_0
203
Réception du premier message M_1 provoquant le recalage de l'horloge interne de la plate-forme réceptrice sur t_r=t1
204
Décodage du premier message M_1 au moyen d'une séquence de décodage DC_1
205
Horloge plate-forme réceptrice
t_r
206
Réception d'un nouveau message $M_?$ dans une fenêtre d'observation temporelle Fn prédéfinie
207
Décodage du message $M_?$ avec une séquence de décodage DCn affectée à la fenêtre de temps Fn

FIG 3

FIG 4


t_e
t_r
M_1
M_2
M_3
M_4
M_5
M_6
F_2
F_3
F_4
F_5
F_6
t1=5h
t1
t2
t3
t4
t5
t6
ΔT_E
ΔT_F

reçue le 07/03/03

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

DÉPARTEMENT DES BREVETS

26 bis, rue de Saint Pétersbourg
75800 Paris Cedex 08
Téléphone : 01 53 04 53 04 Télécopie : 01 42 93 59 30

BREVET D'INVENTION
CERTIFICAT D'UTILITÉ

Code de la propriété intellectuelle - Livre VI

cerfa N° 11235*02

DÉSIGNATION D'INVENTEUR(S) Page N° 1 / 1

(Si le demandeur n'est pas l'inventeur ou l'unique inventeur)

Cet imprimé est à remplir lisiblement à l'encre noire DB 113 W /260899

Vos références pour ce dossier *(facultatif)*	F°A30394/PB/IB
N° D'ENREGISTREMENT NATIONAL	0212404

TITRE DE L'INVENTION (200 caractères ou espaces maximum)
Procédé d'échange sécuritaire de messages d'information.

LE(S) DEMANDEUR(S) :
ALSTOM
25 Kléber
75116 PARIS - FRANCE

DESIGNE(NT) EN TANT QU'INVENTEUR(S) : (Indiquez en haut à droite «Page N° 1/1» S'il y a plus de trois inventeurs, utilisez un formulaire identique et numérotez chaque page en indiquant le nombre total de pages).

Nom		LINARES	
Prénoms		Michel	
Adresse	Rue	Résidence Marceau 26 Rue des Déportés de 1940 à 1945	
	Code postal et ville	92700	COLOMBES
Société d'appartenance *(facultatif)*			
Nom			
Prénoms			
Adresse	Rue		
	Code postal et ville		
Société d'appartenance *(facultatif)*			
Nom			
Prénoms			
Adresse	Rue		
	Code postal et ville		
Société d'appartenance *(facultatif)*			

DATE ET SIGNATURE(S)
DU (DES) DEMANDEUR(S)
OU DU MANDATAIRE
(Nom et qualité du signataire)

Michel GOSSE
Ingénieur Brevets

La loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés s'applique aux réponses faites à ce formulaire.
Elle garantit un droit d'accès et de rectification pour les données vous concernant auprès de l'INPI.